thalesesecurity.com

THALES

VMware and Thales secure the hybrid cloud

Securing data-at-rest wherever it resides

Key benefits:

- Seamlessly migrate and extend on-premises VMware vSphere-based environments to the AWS Cloud
- Achieve compliance with data security mandates for data-at-rest by securing files, volumes and linked cloud storage with encryption, access controls and data access audit logging wherever it resides – across multiple clouds, on-premises and within system, big data and container environments
- Simplify data security administration with centralized key management, encryption and access policies that reach across cloud and data center environments
- Quickly protect existing and new data sets against data breaches without impacting applications, users or operational workflows
- Easily implement privileged user access controls that enable administrators to work as usual, but never be exposed to sensitive data

VMware and Thales secure the hybrid cloud

The problem: the rapid adoption and addition of the cloud is creating a growing need to secure hybrid environments

With more digital initiatives being pursued via the cloud, the mixture of these new cloud offerings with existing on-premises computing has become the new normal. However, just as on-premises and cloud have unique data security challenges, so does this new hybrid model. Challenges such as managing encryption keys from disparate environments and enabling remote key ownership are just a couple of problems to overcome.

vmware®

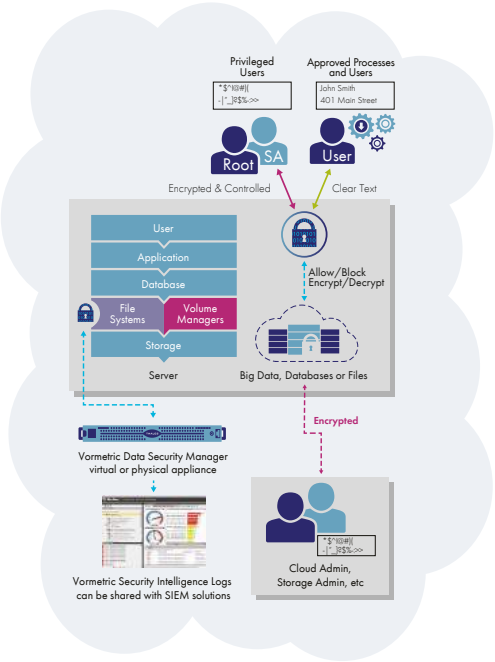

Figure 1 – Vormetric Transparent Encryption encrypts, enforces access policies, and logs all file, volume and linked cloud storage access.

The challenge: protecting more data in hybrid on-premises and cloud environments against more threats

With the rapid adoption of the cloud, safeguarding sensitive data requires much more than just securing a data center's on-premises databases and files. Typical enterprises today use a combination of several on premises and cloud environments that can evolve into further complications resulting from mergers and acquisitions as well as organic application and platform growth. Technologies such as data encryption can help with these challenges but there's also the challenges of dealing with separate key management for each environment or Of course, none of these environments is immune to the increasing number of cyberattacks nor is immune to increasingly strict compliance and regulatory mandates.

VMware and Thales deliver secure hybrid cloud solutions

The solution: VMware Cloud on AWS

VMware Cloud on AWS is an integrated cloud offering that allows you to create vSphere data centers on Amazon Web Services. Highly scalable, secure and innovative, this solution allows organizations to seamlessly migrate and extend their on-premises VMware vSphere-based environments to the AWS Cloud. VMware Cloud on AWS is ideal for enterprise IT infrastructure and operations organizations looking to migrate their on-premises vSphere-based workloads to the public cloud, consolidate and extend their data center capacities, and optimize, simplify and modernize their disaster recovery solutions.

VMware Cloud on AWS can leverage Vormetric Transparent Encryption (VTE) from Thales eSecurity to deliver data-at-rest encryption with centralized key management, privileged user access control and detailed data access audit logging that helps organizations meet compliance reporting and best practice requirements for protecting data, wherever it resides. Transparent Encryption protects structured databases, unstructured files, and linked cloud storage accessible from systems on-premises, across multiple cloud environments, and even within big data and container implementations. Designed to meet data security requirements with minimal disruption, effort, and cost, implementation is seamless – keeping both business and operational processes working without changes even during deployment and roll out.

Why use Thales VTE with VMware cloud on AWS?

Vormetric Transparent Encryption protects data with file and volume level data-at-rest encryption, access controls, and data access audit logging without re-engineering applications, databases or infrastructure. Transparent file encryption deployment is simple, scalable and fast, with agents installed above the file system on servers or virtual machines to enforce data security and compliance policies. Access policies and encryption keys are managed by the Vormetric Data Security Manager, and can span local data centers, cloud environments and hybrid deployments.

Some key advantages are:

- Continuously enforces policies that protect against unauthorized access by users and processes, as well as creating detailed data access audit logs of all activities
- Apply granular, least-privileged user access policies that protect data from external attacks and misuse by privileged users
- Identify and stop threats faster with detailed data access audit logs that not only satisfy compliance and forensic reporting requirements, but also enable data security analytics with popular security information and event management SIEM) systems
- Non-intrusive and easy to deploy. Vormetric Transparent Encryption agents are deployed on servers at the file system or volume level and support both local disks as well as cloud storage environments like Amazon S3 and Azure Files, enabling encryption and access control without requiring changes to applications, infrastructure, systems management tasks or business practices
- Vormetric Transparent Encryption only employs strong, standard-based encryption protocols, such as the Advanced Encryption Standard (AES) for data encryption and elliptic curve cryptography (ECC) for key exchange. The agent is FIPS 140-2 Level 1 validated
- A broad selection of system support, including Windows, Linux, and UNIX platforms, and can be used in physical, virtual, cloud, container and big data environments— regardless of the underlying storage technology. Agents can be located locally on-premises as well as across multiple cloud environments. This agent based architecture eliminates the bottlenecks and latency that plague legacy proxy-based solutions
- Hardware accelerated encryption. Encryption overhead is minimized using the AES hardware encryption capabilities available in modern CPUs (Intel AES-NI, AMD AES-NI, IBM Power8 encryption and Oracle SPARC encryption), delivering encryption with optimal performance even in virtual and cloud environments

About Thales eSecurity

The people you rely on to protect your privacy rely on Thales to protect their data. When it comes to data security, organizations are faced with an increasing amount of decisive moments. Whether the moment is building an encryption strategy, moving to the cloud, or meeting compliance mandates, you can rely on Thales to secure your digital transformation.

Decisive technology for decisive moments.

About VMware

VMware, a global leader in cloud infrastructure and business mobility, helps customers accelerate their digital transformation. VMware enables enterprises to master a software-defined approach to business and IT with VMware Cross-Cloud Architecture™ and solutions for the data center, mobility, and security.

For more detailed technical specifications, please visit www.thalesesecurity.com or www.vmware.com.

Americas – Thales eSecurity Inc. 2860 Junction Ave, San Jose, CA 95134 USA • Tel:+1 888 744 4976 or +1 954 888 6200 • Fax:+1 954 888 6211 • E-mail: sales@thalesesec.com
Asia Pacific – Thales Transport & Security (HK) Lt, Unit 4101-3, 41/F, Sunlight Tower, 248 Queen's Road East, Wanchai, Hong Kong • Tel:+852 2815 8633 • Fax:+852 2815 8141 • E-mail: asia.sales@thales-esecurity.com
Europe, Middle East, Africa – Meadow View House, Long Crendon, Aylesbury, Buckinghamshire HP18 9EQ • Tel:+44 (0)1844 201800 • Fax:+44 (0)1844 208550 • E-mail: emea.sales@thales-esecurity.com